

Cross-border data protection policies for employers

Alison Wetherfield and Melanie Slocombe, McDermott Will & Emery UK LLP

www.practicallaw.com/A48493

The employment relationship is often described in pairs of nouns: master and servant, management and labour, bosses and workers. The last 25 years have added another duo to the list: data controller and data subject.

Employers have always collected and used information which relates to and identifies their employees. However, it has become increasingly important that an employer should not do so, in Europe or in many other parts of the world, without at least some awareness of its obligations to its employees as data subjects under data protection legislation. Most multinationals are likely to want to adopt data protection policies which clearly set out to employees their data protection rights and obligations.

Against this background, this chapter examines:

- The proliferation of data protection legislation.
- Current debate about whether there should be special treatment for employment data processing.
- Implementing data protection employment policies across jurisdictions.
- Practical drafting issues for group-wide data protection policies.

THE PROLIFERATION OF DATA PROTECTION LEGISLATION

In 1980, in response to new technology and increasing data flow among developed countries, the Organisation for Economic Co-operation and Development (OECD) drafted guidelines to reflect and direct an international consensus on basic rules to govern the protection of personal data and privacy (*Basic principles of national applications, Part Two, Annex, OECD Guidelines governing the protection of privacy and transborder flows of personal data 1980 (OECD privacy principles)*) (see box, *The OECD privacy principles*). The ideas incorporated into the guidelines made their way gradually into domestic legislation in many, but not all, OECD member countries (for example in the UK, through the Data Protection Act 1984).

The development which dramatically increased data protection (and the amount of global law on the subject) was the adoption in 1995 of Parliament and Council Directive 1995/46/EC on data protection (Data Protection Directive).

Data protection in Europe

The Data Protection Directive, which applies to EU member states and to the three non-EU countries of the European Economic Area (EEA) (by virtue of the EEA Agreement 1992), took most of the concepts developed by the OECD guidelines and added others. While most existing data protection legislation adopted in response to the OECD guidelines had focused on electronically-processed data, the Data Protection Directive also applies to non-electronic structured sets of personal data.

The OECD guidelines form the basis of a set of core principles for data processing adopted by the Data Protection Directive. But the Data Protection Directive goes much further by imposing a legal framework to reinforce those principles, including requirements to create legal bodies or mechanisms to allow penalties for breaches of data protection principles.

As is usual with EC directives, a wide margin is allowed by the Data Protection Directive for implementation by a member state. The Data Protection Directive also specifically allows member states to distinguish between types of data and to either prohibit, or allow only on a very restricted basis, processing of special categories of data which reveal:

- Racial or ethnic origin.
- Political opinions.
- Religions or philosophical beliefs.
- Trade union membership.
- Health or sex life.
- Offences or criminal convictions.

The implementation of the Data Protection Directive across the member states (now 25) provides a good illustration of the strengths and problems of a framework approach. The basic data protection principles are well understood and uniform across Europe. The problem is that the legal bodies and mechanisms for policing them vary greatly across member states.

The precise preconditions for processing data also vary, particularly for data where enhanced protection is allowed by the Data Protection Directive. Any data controller with establishments in more than one member state, or with a need to pass data to other entities in other member states, therefore needs to understand the similarities and differences. A data controller familiar with the UK's legislation implementing the Data Protection Directive,

THE OECD PRIVACY PRINCIPLES

The following principles, first stated in 1980, form the core of most data protection laws around the world (*Basic principles of national application, Part Two, Annex, OECD Guidelines governing the protection of privacy and transborder flows of personal data 1980*).

Collection limitation

There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data quality

Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and kept up to date.

Purpose specification

The purposes for which personal data are collected should be specified no later than at the time of data collection. The subsequent use of such data should be limited to fulfilling these purposes (or purposes compatible with them), and any change of purpose should be specified.

Use limitation

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified according to the purpose specification principle except either:

- With the consent of the data subject.
- By the authority of law.

Security safeguards

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness

There should be a general policy of openness about developments, practices and policies in relation to personal data. Means should be readily available for establishing the:

- Existence and nature of personal data.
- Main purposes of its use.
- Identity and usual residence of the data controller.

Individual participation

An individual should have the right to:

- Obtain from a data controller, or equivalent, confirmation of whether the data controller has data relating to him.
- Have data relating to him communicated to him:
 - within a reasonable time;
 - at a charge, if any, that is not excessive;
 - in a reasonable manner;
 - in a form that is readily intelligible.
- Be given reasons if a request made under the two bullet points above is denied and to be able to challenge such a denial.
- Challenge data relating to him and, if the challenge succeeds, to have the data erased, rectified, completed or amended.

Accountability

A data controller should be accountable for complying with measures which give effect to all the above principles.

the Data Protection Act 1998, is likely to be surprised by the different choices on implementation and derogation taken in some other European jurisdictions (*see below, Practical drafting issues for group-wide data protection policies*).

This need to be aware of the laws of other jurisdictions does not only apply within Europe. One of the most controversial aspects of the Data Protection Directive is a provision which has affected the discussion and adoption of data protection legislation far beyond Europe.

The effect of EC data protection law on the rest of the world

Article 25 of the Data Protection Directive prohibits the transfer of personal data from inside the EEA to countries that do not

ensure adequate levels of protection. Adequacy is assessed on a case-by-case basis in light of all the circumstances surrounding a data transfer operation. These specifically include all relevant legal provisions, both general and sectoral, in force in the relevant third country. Article 26 sets out some derogations and exceptions to this rule (including where the data subject has given unambiguous consent), and allows the European Commission to approve both specific third countries and methods to allow specific transfers.

Article 25 in effect demands all member states to require data controllers in their jurisdiction to know about and assess the systems for data protection in the third countries they wish to send data to (without actually requiring the domestic legislation of EU member states to be applied outside the member state).

IMPLEMENTING A DATA PROTECTION POLICY IN DIFFERENT EUROPEAN JURISDICTIONS

Country	What needs to be done to implement a policy for existing employees?	What needs to be done to implement a policy for new employees?
Finland	Provide sufficient notification to existing employees about the content of the data protection policy and ask them to sign the policy.	Incorporate the policy into the contract of employment by reference and require the employee to sign the policy.
France	<p>In relation to the parts of the policy that deal with employees' compliance:</p> <ul style="list-style-type: none"> ■ Incorporate these into the existing company rules and regulations. ■ File the amended rules and regulations in duplicate with the labour inspector, together with works council/staff delegates' opinion on the documents. ■ File the document with the clerk of the local industrial tribunal. ■ Display the document at the company's premises. <p>In addition, notify existing employees about the content of the policy and explanatory notice, and ask them to sign the policy.</p>	<p>Standard employment contracts should have provisions where employees consent to processing and transfer outside the EU.</p> <p>Employees should also be provided with a copy of, and be asked to sign, the policy. An explanatory notice should also be provided.</p>
Germany	Issue a supplement to employment contracts attaching a copy of the policy, both of which must be signed and returned. The supplement should be signed twice (one signature for the supplement itself and one for consent in relation to data protection).	Incorporate the policy into the employment contract by reference and ask the new employee to sign the policy.
Italy	<p>Amend the internal corporate regulations established by the employer in Italy, to refer to the policy and to confirm that the policy is contractually binding on employees.</p> <p>Notify all employees of new internal corporate regulations by displaying them, with the policy, in a place accessible to everyone, and by delivering the policy to each employee.</p> <p>If the employer in Italy has no internal corporate regulations, display the policy, with an extract of the disciplinary rules and relative penalties of any relevant national collective agreement, in an accessible place, and deliver them to each employee.</p>	Provide employees with a copy of the internal regulations (if any) or the policy, together with an extract of the disciplinary rules and relative penalties of any relevant national collective agreement.
The Netherlands	Provide sufficient notification to existing employees about the content of the policy and ask them to sign it.	Incorporate the policy into the employment contract by reference and ask the employee to sign it.
Spain	Provide sufficient notification to existing employees about the content of the policy and ask them to sign it.	Incorporate the policy into the employment contract by reference and require the employee to sign the policy.
Sweden	Provide sufficient notification to existing employees about the content of the policy and ask them to sign it.	Incorporate the policy into the employment contract by reference and require the employee to sign the policy.
UK	Provide sufficient notification to existing employees about the content of the policy and ask them to sign it.	Incorporate the policy into the employment contract by reference and require the employee to sign the policy.

Cross-border

Does a works council or trade union need to be involved?	Is a translation required from English into the native language?
Not when the number of employees is less than 30.	No.
Yes, the draft policy must be submitted to the works council (if there is one) to provide staff representatives with sufficient information to express an opinion. If the conditions for setting up a works council have not been met, there is no duty to inform staff delegates, unless the processing of data by electronic means involves replacing paper files, registers or mandatory documents to which staff delegates must be allowed access.	Yes.
If there is a works council or trade union, its consent is required.	Yes.
No.	Yes.
If the employer in The Netherlands has established a works council (which is only required if it has 50 or more employees), the approval of the works council is required before asking employees to consent to the policy.	No, provided the employee understands English.
No.	Not a legal requirement, but it is recommended.
No.	No, provided the employee understands English.
No.	No.

This challenge has been met in different ways across Europe. The UK, for example, allows individual data controllers to assess whether there is an "adequate level of protection" for any given transfer without seeking prior consent from the Information Commissioner (the government body with data protection oversight and enforcement powers) or securing express consent from a data subject. In other member states, for example Italy, express consent for an overseas transfer from the data subject must be secured (although this is frequently ignored).

Reactions from non-European countries to Article 25 have included hostility to the perceived arrogance of the EU in judging the data protection laws of third countries. So far, the EU has only approved the data protection legal regimes of a handful of jurisdictions, notably Argentina, Canada, Hungary and Switzerland. The US has no overall approval, although the safe harbour scheme devised by the Federal Trade Commission provides limited protection for transfers to the US for the small number of companies which have signed up to the scheme.

Some non-European jurisdictions appear to have reluctantly accepted that, if Europe insists on certain standards being met outside the EU, this has to be done for commercial reasons. For example in November 2004, the 21 member states of the Asia-Pacific Economic Cooperation (APEC) forum (which include Australia, Japan, Korea, Malaysia, New Zealand, Thailand and the US) endorsed a privacy framework with objectives to:

- Develop appropriate privacy protections for personal information.
- Prevent the creation of unnecessary barriers to information flows.
- Enable multinational businesses to implement uniform approaches to the collection, use and processing of data.
- Facilitate both domestic and international efforts to promote and enforce information privacy protections.

The new APEC Privacy Framework calls on member states to hold data controllers accountable for complying with principles based on the OECD guidelines. While it has been criticised as being a watering down of the original OECD principles for the Asia-Pacific region, it is likely to lead to more data protection laws being adopted by APEC members (although most already have some legislation). This is yet more law which global data controllers, including multinational employers, must comply with.

SHOULD THERE BE SPECIAL TREATMENT FOR EMPLOYMENT DATA PROCESSING?

All the above data protection legislation and initiatives can be described as one size fits all. There is no special provision in the OECD guidelines, the Data Protection Directive or the APEC Privacy Framework for the special position of employers as data controllers and employees as data subjects.

Representatives of both employers and employees have, however, been discussing whether there should be special provision. The standing advisory committee to the EC on data protection (the Article 29 Working Party) has rather controversially given the

opinion that while consent of a data subject can usually be relied on to establish the lawfulness of processing by a data controller, reliance on consent in the employment context should be confined to cases where the worker has a genuine free choice (*Opinion 8/2001 on the processing of personal data in the employment context*).

The Article 29 Working Party and many representatives of organised labour are clearly sceptical about how much, if any, free choice employees have in a relationship where employers have more power than employees. As unambiguous consent is one of the ways to ensure the legality of transfers of data outside the EEA, this is an opinion of potentially huge significance to multinational employers.

The International Chamber of Commerce (ICC) also thinks that data processing is different in the employment context, but takes a predictably different view on the issue of employee consent. The ICC notes that "consumers routinely consent to contractual provisions that they have no opportunity to negotiate, and consent in this context is not considered invalid unless the terms are unduly burdensome or onerous. The same should hold true for employees" (*Part III, ICC policy statement on employee privacy, data protection and human resources, December 2003 (ICC policy statement)*).

This ICC policy statement also warns against too many data protection regimes, and suggests that "the lack of clarity for both employers and employees of the many national policies and laws on workplace privacy is creating an unacceptable level of risk for businesses, particularly multinational business ... greatly increas[ing] companies' compliance burden without appreciably improving employees' privacy" (*Part I, ICC policy statement*).

On data transfer in the employment context, the ICC makes a strong case for allowing multinational companies to develop unified and comprehensive systems for human resource data management. In particular, it recommends corporate codes, applying to employees globally, without cumbersome registration and notification procedures and with a streamlined approval process.

So far, these calls have not led to any specific legislation or guidance at EU level (although the Information Commissioner in the UK clearly sees such processing as sufficiently unique to justify the production of the Employment Practices Code, a 90-page guidance on data processing good practice). However, during 2005 it is likely that the European Commission will produce an initiative on data protection in employment.

IMPLEMENTING DATA PROTECTION EMPLOYMENT POLICIES ACROSS JURISDICTIONS

Employer and employee representatives are hoping that the EU will decide how multinational employers can ensure that their intra-group transfers of employee data from the EEA to third countries satisfy Article 25. While unambiguous consent can theoretically be sought from employees for this (and often is in employment contracts), consent is a controversial area (see above, *Should there be special treatment for employment data processing?*).

The ICC's reference to corporate codes of conduct is relevant here because the Article 29 Working Party has, since 2003, been experimenting with a new method to satisfy Articles 25 and 26, called binding corporate rules. These would remove any need for consent from individual data subjects. The Article 29 Working Party has stated that one national data protection regulator in the EC should be able to approve the binding corporate rules as satisfying Article 25, wherever the data is to be transferred in the world, if all of the following are met:

- A multinational adopts binding corporate rules about how it will process data, wherever it is located in the world.
- The binding corporate rules are legally enforceable by data subjects, including those in the EU.
- A checklist of points set out on 14 April 2005 is satisfied (see box, *The Article 29 Working Party approval procedure*).

Following one such approval, a multinational employer would be able to apply the data protection policy in other EU member states, without having to seek permission from each data protection regulator, and without seeking individual consent.

Multinationals already have an incentive, given the similarity of data protection principles developing around the world, to develop uniform policies for employees worldwide. Such policies, when carefully drafted, can serve a number of purposes, for example:

- Informing employees of the types of data relating to them that the employer will process, and of the types of processing (which may involve disclosure to third parties).
- Stating general adherence to the data protection principles.
- Seeking specific consent (where the law allows) for processing sensitive personal data, and for transferring data for specific employment purposes outside the EEA. Consent is usually sought by incorporating the policy into individual employment contracts.
- Requiring employees acting as agents of the employer to handle data managed by them during employment according to data protection principles (including data relating to non-employee data subjects such as individual clients or suppliers).

The binding corporate rules development gives multinationals a chance to get protection against an EU employee claim for a breach of Article 25, by using a policy that they would probably develop in any case to satisfy different data protection obligations. However, this is a new development. While many multinationals are developing uniform privacy policies worldwide, none have yet successfully adopted binding corporate rules which have satisfied the proposed Article 29 Working Party approval procedure (although GE, Phillips and DaimlerChrysler are all working on it) (see box, *The Article 29 Working Party approval procedure*).

PRACTICAL DRAFTING ISSUES FOR GROUP-WIDE DATA PROTECTION POLICIES

Any group-wide data protection policy will need some tailored drafting. It will be slightly different across jurisdictions, even in Europe, as shown by the following examples (unless it is so high level as to not actually inform employees of jurisdiction-specific rights and obligations).

Processing sensitive personal data

Sensitive personal data is generally that relating to all of the following:

- Race and ethnic origin.
- Political opinions or religious beliefs.
- Membership of a trade union.
- State of health.
- Sexual life.
- Commission or alleged commission of an offence.

Generally, the express, informed consent of the individual is required to process sensitive personal data. If the employer does process such data, the data protection policy will usually explain the limited use planned for it and require consent. However:

- Spain distinguishes between information relating to religious beliefs and trade union membership (for which express written consent is needed), and information about racial origin, health or sexual life, which must only be processed if legally required, regardless of consent.
- In Austria, Italy and Portugal, there are specific requirements to get prior clearance from the relevant data protection registrars before processing sensitive personal data.
- In certain countries, it is expressly forbidden to collect and process certain sensitive personal data, for example:
 - in Belgium, data relating to philosophical, religious, and union beliefs, except for the benefit of the employee;
 - in Italy, data relating to religious and political opinions.

Retention and accuracy of data

There is a general principle across Europe that, although there are no specific time limits on retaining personal data, such data should only be kept as long as necessary. The data protection policy should provide that data will only be retained for the purposes described and for so long as necessary, as appropriate to the employment relationship or to comply with a legal obligation.

Any data protection policy should also provide that the employer will take all reasonable steps to ensure that information is kept up to date and is accurate. However, in:

THE ARTICLE 29 WORKING PARTY APPROVAL PROCEDURE

The procedure suggested by the Article 29 Working Party for implementing a set of binding corporate rules is in two stages.

Stage 1: draft proposals

Organisations initially need to propose a scheme which will both:

- Be legally binding.
- Provide an adequate level of protection for personal data.

As a minimum, the rules or code of conduct must adhere to the protections placed on personal data by Parliament and Council Directive 1995/46/EC on data protection (Data Protection Directive).

Stage 2: approval process

The draft rules must then be submitted for approval to the most appropriate national regulator (in the UK, the Information Commissioner). While the data protection authority to which the application is sent decides which data protection authority is the most appropriate, factors to consider include the member state:

- In which the organisation has its European headquarters.
- In which the company with delegated data protection responsibilities is situated (for example, if the organisation does not have a European headquarters).
- From which most transfers to outside the EEA will take place.

For organisations with a presence in a large number of jurisdictions, implementing binding corporate rules has one major advantage, namely that the organisation only needs to submit its proposals to a data protection authority in one member state.

After submission, the relevant regulator reviews the draft rules and liaises with its counterparts in other European member states to obtain approval from all the authorities concerned. Currently, no one member state can approve the draft rules without consulting other member states. This inevitably delays the process.

Model checklist and co-operation procedure

On 14 April 2005, the Article 29 Working Party adopted two working documents about using binding corporate rules to transfer personal data within a group of companies and outside the EEA.

A co-operation procedure was adopted, detailing how to submit a code for approval by the various data protection authorities, and how they will co-operate with each other when considering the application.

A model checklist was also adopted (based on a draft checklist created by the UK's Information Commissioner), setting out what an application should contain to obtain approval. A summary of the key elements is set out below:

- **Information required.** This includes contact details, a background paper summarising how the required elements have been satisfied and all relevant documents comprising the binding corporate rules to be adopted.
- **Evidence that the measures are legally binding and how this is achieved.** This applies both within the organisation (in relation to employees, subcontractors and members of the group) and externally for the benefit of individuals.
- **Remedies and sanctions available.** Details must be provided of the practical steps a data subject can take to obtain a remedy and the penalties imposed if there is a breach.
- **Verification of compliance.** Details of audit arrangements (both internal and external) must be provided.
- **Description of processing and flow of information.** The draft rules must identify all of the following:
 - nature of the data;
 - purposes for which it is processed;
 - extent of the transfers within the group;
 - whether all transfers between group members are covered (or only those from the EU).

Details should also be provided of the basis on which onward transfers of data will take place.

- **Data protection safeguards.** Applicants must ensure that their draft rules contain a clear description of how the standards set out in the Data Protection Directive are met within the organisation.
- **Mechanism for reporting and recording changes.** Procedures must be in place for notifying any changes, both within the organisation and to the relevant data protection authority.

- Finland and Switzerland, the starting point is that data should be destroyed once an employee leaves, unless it is still needed (in any event in Switzerland, data should not be kept for more than five to ten years).
- Belgium, a time limit of no more than ten years is recommended.
- Denmark, France and the Netherlands, the employer must notify the local data protection regulator of what data they intend to keep and the cut-off dates to be used. In France, there is a penalty of imprisonment for up to three years and a fine of up to EUR225,000 (about US\$290,000) for non-compliance with this requirement.

Rights of access

There is a general principle across Europe that an individual can make a subject-access request. This means an employee can essentially obtain data held on them by the employer. The data protection policy should note that the employer will comply with subject-access rights, but there are country-specific rules as to how this access happens (for example, how often an employee

can request the data and how much it costs). For example in:

- The UK, employees can make such requests at reasonable intervals and must pay GB£10 (about US\$19). The employer must reply within 40 days.
- The Czech Republic, the employee can make the request once a year, free of charge.
- Poland, the request can be made at reasonable intervals.
- France and Switzerland, the request is free of charge.

Practical implementation issues for group-wide data protection policies

Just as drafting is likely to require consideration of slightly different approaches in some jurisdictions, so too will implementation. Again, advice is needed on a jurisdiction-by-jurisdiction basis (*for an overview of key EU jurisdictions, see table, Implementing a data protection policy in different European jurisdictions*).

PRACTICAL LAW COMPANY

PLC Cross-border

e-mail

Keep up to date with all new content added to ^{PLC}Cross-border, including all of the material highlighted in this handbook, by signing up for our monthly e-mail at:

www.practicallaw.com/emailpreferences

The e-mail details new and updated resources added to the site in the preceding month including features, handbooks and practice manuals (containing practice notes, standard documents and checklists) as well as upcoming Practical Law Company events.